PATENT ABSTRACTS OF JAPAN

(11)Publication number : 09-247086
(43)Date of publication of application : 19.09.1997

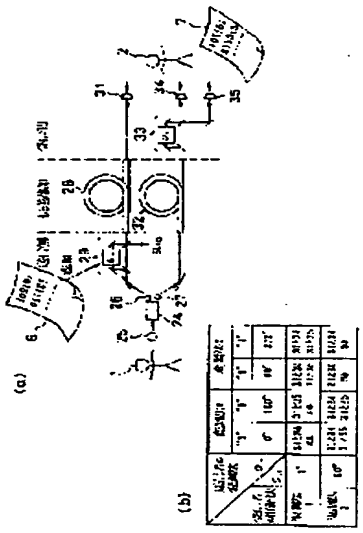
(51)Int.Cl. H04B 10/00
G01J 9/00
G02F 1/39
G09C 1/00
H04L 9/08
H04L 9/38

(21)Application number : 08-052102
(22)Date of filing : 08.03.1996

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>
(72)Inventor : IMOTO NOBUYUKI
KOASHI MASATO
MAIKERU UERUNAA

(54) CONSTITUTION METHOD FOR QUANTUM PASSWORD

(57)Abstract:
PROBLEM TO BE SOLVED: To provide the constitution method of a quantum password, which does not require a highly precise synchronous clock, by using a remote quantum correlation without using polarization and executing simultaneous measurement only on a receiver-side.
SOLUTION: A transmitter 1 generates photons 26 and 27 from a pump photon 25 by using an optical parametric amplifier 24. The photon 26 is transmitted to an optical fiber 28 after it passes through a delay 29 and the photon 27 is transmitted to an optical fiber 32. On a reception-side, the photon 26 is counted in a light receiver 31 and the photon 27 is counted in a light receiver 34 or 35 after it passes through a delay 33. The signals are simultaneously counted in the light receiver 31 and the light receiver 34 or 35. Whether a phase difference which the delay 29 gives and that which the delay 33 gives are a specified combination or not is recognized by a classic channel. Only when it is the specified combination, the signal of one bit is registered.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁(JP)　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平９－２４７０８６

(43)公開日　平成9年(1997)9月19日

(51)Int.Cl.[6]		識別記号	庁内整理番号	FI			技術表示箇所
Ｈ０４Ｂ	10/00			Ｈ０４Ｂ	9/00	Ｚ	
Ｇ０１Ｊ	9/00			Ｇ０１Ｊ	9/00		
Ｇ０２Ｆ	1/39			Ｇ０２Ｆ	1/39		
Ｇ０９Ｃ	1/00	６３０	7259－５Ｊ	Ｇ０９Ｃ	1/00	６３０　Ｃ	
			7259－５Ｊ			６３０　Ｚ	

審査請求　未請求　請求項の数３　ＯＬ　（全１１頁）最終頁に続く

(21)出願番号　特願平8-52102

(22)出願日　平成8年(1996)3月8日

(71)出願人　000004226
日本電信電話株式会社
東京都新宿区西新宿三丁目19番2号

(72)発明者　井元　信之
東京都新宿区西新宿三丁目19番2号　日本電信電話株式会社内

(72)発明者　小芦　雅斗
東京都新宿区西新宿三丁目19番2号　日本電信電話株式会社内

(72)発明者　マイケル・ウェルナー
東京都新宿区西新宿三丁目19番2号　日本電信電話株式会社内

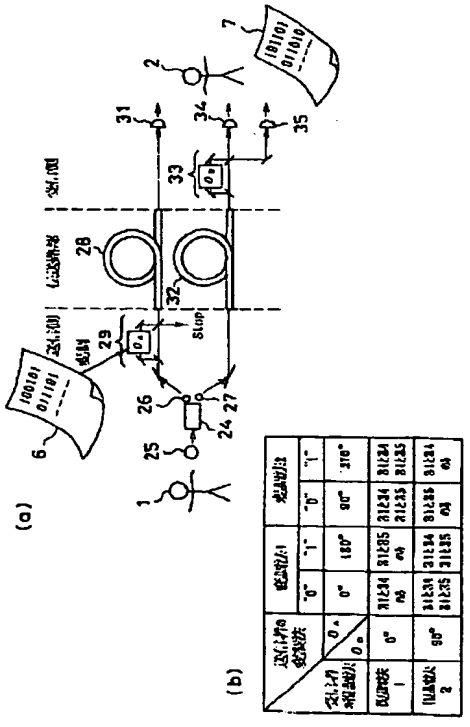
(74)代理人　弁理士　三好　秀和　(外1名)

(54)【発明の名称】量子暗号の構成方法

(57)【要約】

【課題】　偏光を使用せず、遠隔量子相関を利用し、同時刻性測定を受信者側のみで行うことにより高精度同期クロックを必要としない量子暗号の構成方法を提供する。

【解決手段】　送信者１は光パラメトリック増幅器２４を用いてポンプ光子２５から光子２６，２７を発生し、光子２６は遅延２９を通過後光ファイバ２８に送り、光子２７は光ファイバ３２に送る。受信側で光子２６を受光器３１でカウントし、光子２７は遅延３３を通過後受光器３４または３５でカウントする。受光器３１と受光器３４または３５で信号が同時にカウントされ、しかも遅延２９が与える位相差と遅延３３が与える位相差が特定の組合せであったか否かを古典チャンネルにより確認し、特定の組合せであった場合のみ、１ビットの信号を登録する。



1

【特許請求の範囲】

【請求項１】　量子力学状態を変調した第１の信号を伝える量子チャンネルと、古典状態を変調した第２の信号を伝える古典チャンネルを用い、不確定性原理に基づいて盗聴行為によって前記第１の信号に発生する撹乱の有無を前記古典チャンネルで監視しながら、乱数表を送信側より受信側に伝送し、前記乱数表を秘密鍵とする量子暗号の構成方法において、

送信側において、同一の時間幅を有し、前記時間幅より長いコヒーレント時間を有し、それぞれが１つの光子からなる第１および第２の光パルスを発生し、

前記第１の光パルスを２つの光路に分岐し、分岐後の光パルスの一方に前記時間幅より長く前記コヒーレント時間より短い第１の時間遅延を施した後、分岐した他方の光パルスの光路に合流させ、合流した光路が取り得る２つの光路のうちの１つの光路を第１の量子チャンネルに光学的に接続し、

前記第２の光パルスを第２の量子チャンネルに入力し、

受信側においては、前記第１の量子チャンネルの出力を第１の光検出手段に入力し、

前記第２の量子チャンネルの出力を２つの光路に分岐し、分岐後の光パルスの一方に、前記第１の時間遅延との差が前記時間幅より小さい第２の時間遅延を施した後、分岐した他方の光パルスの光路に合流させ、合流した光路が取り得る２つの光路の一方を第２の光検出手段に入力し、他方の光路を第３の光検出手段に入力し、

前記第１の光検出手段と第２または第３の光検出手段で信号が同時に検出され、しかも前記第１の時間遅延が与える位相差と第２の時間遅延が与える位相差が特定の組合せであったか否かを古典チャンネルにより確認し、特定の組合せであった場合のみ、１ビットの信号を登録することを特徴とする量子暗号の構成方法。

【請求項２】　前記第１および第２の光パルスを光パラメトリック増幅または原子のカスケード遷移によって発生することを特徴とする請求項１記載の量子暗号の構成方法。

【請求項３】　量子力学状態を変調した第１の信号を伝える量子チャンネルと、古典状態を変調した第２の信号を伝える古典チャンネルを用い、不確定性原理に基づいて盗聴行為によって前記第１の信号に発生する撹乱の有無を前記古典チャンネルで監視しながら、乱数表を送信側より受信側に伝送し、前記乱数表を秘密鍵とする量子暗号の構成方法において、

送信側において、ポンプ光子を光パラメトリック増幅器に供給して、第１の光パルスおよび第２の光パルスを発生し、

第１の光子パルスを２つの光路に分岐し、分岐された一方の光パルスに遅延手段で第１の時間遅延を施し、分岐した他方の光パルスの光路に合流させ、合流した光路が取り得る２つの光路のうちの１つの光路を光ファイバからなる第１の量子チャンネルに光学的に接続し、

2

前記第２の光パルスを光ファイバからなる第２の量子チャンネルに入力し、

受信側においては、前記第１の量子チャンネルの出力を第１の受光器に入力し、

前記第２の量子チャンネルの出力を２つの光路に分岐し、分岐された一方の光パルスに遅延手段により第２の時間遅延を施し、分岐した他方の光パルスの光路に合流させ、合流した光路が取り得る２つの光路の一方を第２の受光器に入力し、他方の光路を第３の受光器に入力し、

前記第１の受光器と第２または第３の受光器で信号が同時に検出され、しかも前記第１の時間遅延が与える位相差と第２の時間遅延が与える位相差が特定の組合せであったか否かを古典チャンネルにより確認し、特定の組合せであった場合のみ、１ビットの信号を登録することを特徴とする量子暗号の構成方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、量子力学の不確定性原理を利用し、盗聴者に有無をモニタしながら鍵である乱数列を交換する量子暗号の構成方法に関する。

【０００２】

【従来の技術】暗号には、盗聴されていることを前提にその解読が計算量論的に困難であることに安全性の根拠を置く現代暗号と、量子力学の不確定性原理を利用し、盗聴者の有無をモニタしながら鍵である乱数列を交換することを特徴とする量子暗号とがある。まず、現代暗号について説明する。

【０００３】現代暗号は、送信するメッセージを数字化し（これを平叙文と呼ぶ）、それに乱数を演算して第三者にはランダムに見える暗号文にし、第三者の知らない復号法で受信者が復号するもので、大きく分けて秘密鍵暗号法と公開鍵暗号法がある。送信者が暗号化に使う乱数表を暗号鍵、受信者が復号に使う乱数表を復号鍵と呼ぶが、秘密鍵暗号法では暗号鍵と復号鍵は同一（秘密鍵と呼ばれる）であり、送信者と受信者は何らかの安全な方法、例えば直接会うなどで事前に秘密鍵を決定している。

【０００４】平叙文と秘密鍵の長さが等しいとき、すなわち一度使った秘密鍵は必ず捨てるとき（これをone time pad法と呼ぶが）、この方法は絶対的安全性を有していることがShannon により証明されている。しかし、メッセージに匹敵する長さの秘密鍵をその都度事前に交換することの非現実性（それができるならばメッセージそのものを交換すればよい）の故、one time pad法は実際には使われていない。実用的な秘密鍵暗号法では同じ秘密鍵を繰り返し使用する。

【０００５】公開鍵暗号法では受信者が公開鍵と秘密鍵の２つを所有しており、公開鍵を一般に公開する。送信

者は受信者の公開鍵を使って暗号化し送信し、受信者は秘密鍵を使って復号化する。いうまでもなく、ここでも公開鍵と秘密鍵を繰り返し使用する。これらの現代暗号については文献：［１］太田和夫・黒澤馨・渡辺治著「情報セキュリティの科学」（講談社ブルーバックス）、［２］今井秀樹著「暗号のおはなし」（日本規格協会）、［３］岡本英司著「暗号理論入門」（共立出版）、［４］池野信一、小山謙二著「現代暗号理論」（電視通信学会）に詳しく説明されている。

【０００６】現代暗号では暗号文が盗聴されることを前提としており、盗聴されても解読に天文学的時間がかかることに安全性の根拠を置いている。計算量論的表現を用いれば、整数の素因数分解がＰ型問題に属していないという仮説に根拠を置いている。

【０００７】しかし、この仮説は未だ証明されていない予想に過ぎない。それどころか１９９４年には量子コンピューティング法まで計算法を拡張すれば、素因数分解がＰ型問題に転化さることが数学的に証明された。これについては文献：［５］Peter W.Shor:"Algorithms for quantum computation:Discrete logarithms and factoring,"Proceedings of the 35th Annual Symposium on Foundations of Computer Science,edited by S.Goldwasser (IEEE Computer Society,Los Alamitos,CA,1994) p.124 、［６］西野哲朗「量子コンピュータ」情報処理学会誌第３６巻４号（1995年 4月）p.337 に詳しく説明されている。

【０００８】この量子コンピュータは未だ実用化されていないが、現代暗号の究極の拠り所が理論上とはいえ崩れ去ったため、その安全性が将来保証されなくなることが避けられないと考えられている。

【０００９】次に、従来の量子暗号について説明する。

【００１０】量子コンピューティング法を用いても、なお破ることができない暗号として量子暗号がある。これは量子力学の不確定性原理に基づき盗聴者のどんな盗聴行為も必ず何らかの痕跡を量子レベルの信号に残すことを利用し、盗聴されていないことを確認しながら秘密鍵を決定する手続きである。すなわち、上述した秘密鍵暗号方式において送信者と受信者が何らかの安全方法で事前に秘密鍵を決定しておく必要があるが、その安全な方法としては、直接会見を除けば現在のところ量子暗号以外はない。量子暗号を用いれば恒常的に秘密鍵の交換を行うことが可能であり、絶対安全が保証されているone time pad法の使用が可能となる。

【００１１】量子暗号の具体的方法として４偏光状態暗号、２コヒーレント状態暗号、４コヒーレント状態暗号、時間差干渉暗号、二光子干渉暗号が提案されている。次に、これらの各量子暗号について説明する。

【００１２】まず、４偏光状態暗号について説明する。４偏光状態暗号は最初に考案された量子暗号であり、詳細は文献：［７］C.H.Benett and G.Brassard,in Proceedings of IEEE International Conference on Computers,Systems and Signal Processing,Bangalore,India (IEEE,New York,1984) ,p.175、［８］Ａ．エカート／井元信之訳「量子暗号への招待」パリティ、vol.7,No.2,p.26 (1992)、［９］Ｇ．コリンズ／井元信之訳「量子暗号は史上最強の暗号」パリティ、vol.8,No.5,p.31 (1993) に述べられているが、以下簡単に説明する。

【００１３】４偏光状態暗号においては、図２に示すように、送信者１と受信者２は１ビットにつき光子を１つだけ含む光パルス３を送る量子チャンネル４と送信および受信状況を確認し合う古典的チャンネル５を使う。量子チャンネル４は通常光ファイバであり、古典的チャンネル５は無線や電話等である。古典的チャンネル５は盗聴されていることを前提とするが、改竄はされないと仮定する。このことを明確にするため、以下本明細書では古典的チャンネルを公開チャンネルと呼ぶ。また、量子暗号に限らず暗号理論の前提として、盗聴者は図の伝送路部にアクセスすることはできるが、送信側および受信側にはアクセスできない。送信側ビット“０”および“１”を光パルス３にコーディングするにあたり、直線偏光と円偏光の２種類の変数、すなわち２種類のコーディング法を用いる。例えば、図３に示すように、直線偏光コーディングの場合は「水平」を“０”に、「垂直」を“１”に、円偏光コーディングの場合は「右回り」を“０”に、「左回り」を“１”に対応させる。このような取り決めを送信者１と受信者２は予め（公開チャンネル５で）行っておく。送信者１は二進法で書かれた乱数表６を用意する。これは受信者２と共有する秘密鍵７を生成するための元になる乱数表である。秘密鍵７は次に説明するように乱数表６から半分弱のビットを抽出した部分乱数表となっている。４偏光状態暗号における送信者１と受信者２のプロトコルは次のようになる。

【００１４】ステップ１：送信者１はランダムにコーディング法を選択し、乱数表６に従って光パルス３の偏光を変調器８を用いて変調する。例えば円偏光でコーディングすることとし、乱数表６の最初の値が“１”ならば「左回り」偏光となるように光パルス３の偏光状態を変える。送信者１には選択したコーディング法は知らせず、光パルス３だけを送る。同様にして引き続くビットに対して次々と光子を送る。

【００１５】ステップ２：受信者２は受けた光パルス３が光子を１つしか含まないので、直線偏光と円偏光の両方を測ることはできない（不確定性原理）。従って、どちらを測るかを決心し、偏光測定器を含む受光器９を用いて測定する。送信者１が選択したコーディング法と同じコーディング法と間違ったコーディング法を選ぶ確率はそれぞれ５０％である。同じだった場合、乱数表６の値が正しく受信者２に再現されるが、間違った場合はそのビットに関する送信者１と受信者２の間の相互情報量

はゼロとなる。

【００１６】ステップ３：光パルスを１つ測定する毎に（あるいは後でまとめて交信してもよいが）受信者２はどちらのコーディング法を選択したか、公開チャンネル５で明らかにする。送信者１はそれを聞き、受信者２のコーディング選択が正しかったか否かを公開チャンネル５で伝える。

【００１７】ステップ４：送信者１と受信者２は双方が同じコーディング法を選択した約半分のビットだけを採用し、後の半分は捨てる。盗聴がなければ双方に同じ乱数表が形成されているはずである。

【００１８】ステップ５：送信者１と受信者２は残ったビットのうち適当な割合で照合ビットを抽出し、それぞれの答合わせを（公開チャンネル５で）行う。十分な数の照合ビットが一致すれば、上記文献に説明されているような理由により、１に近い確率で盗聴されていないと結論づけられる。

【００１９】ステップ６：照合ビットも除いたビットは送信者１と受信者２しか知らない同一の値を有することが保証されているので、それを秘密鍵７と決定する。

【００２０】以上の手順により、盗聴されていないことをリアルタイムでモニタしながら秘密鍵を生成して行くことができる。万一照合ビットから盗聴を発見した場合は、盗聴発見期間の交信をすべて無効とし、量子チャンネルをチェックするか、あらためて構築する。実際は盗聴者が最も恐れるのは盗聴の発覚であり、しかも発覚の危険を侵しても盗聴遂行できない（盗聴した秘密鍵は破棄されてしまう）ので、量子暗号に対して盗聴者のなすべき手段は事実上ない。

【００２１】なお、量子暗号の実用性を示す特徴の１つとして、伝送路損失の存在が致命的でないという事情についてここで触れておきたい。光の量子状態を制御する通信や情報処理においては伝送路の損失あるいは光検波器の不完全な量子効率により量子状態が大きく破壊されてしまうことが致命的欠陥であることが知られている。意味を持つメッセージを送信したり処理したりする場合は、量子状態の破壊は情報そのものの破壊を意味する。しかし、量子暗号はまず乱数表の交換が目的であるので、伝送損失等により光子が欠落しても乱数表が間引きされるに過ぎない。損失の影響は主に伝送レートが下がることに現れるだけであり、上記プロトコルの有効性には影響しない。このような特徴は４偏光状態暗号に限らず、量子暗号すべてに共通する特徴である。

【００２２】４偏光状態量子暗号を実用化する際に最も重要となるのは、光子が伝送路を通過する間に予測不能な偏光の撹乱があってはならないことである。この撹乱を避けるためにいわゆる偏光保存ファイバを用いることはできない。偏光保存ファイバは直交する特定の２つの偏光を保存するだけであり、４偏光状態暗号で用いられるような直交しない組合せも含む４つの偏光をすべて保存することはできない。一方偏光を保持しないファイバは偏光の時間的揺らぎが避けられない。揺らぎを時間追跡して偏光補償する技術はあるが、ただ１つの光子を送受信する場合には適用できない。送信偏光が受信偏光に誤って伝えられた場合、照合ビットの矛盾と秘密鍵生成エラーの原因となる。すなわち、照合ビットの矛盾が発見された場合、測定誤りと盗聴による２つの原因を峻別しなければならないが、それは一般に困難であり、複雑な誤り訂正手続きの導入が避けられない。更に盗聴でなく測定誤りと判定され秘密鍵を破棄しない場合も、測定誤りによる秘密鍵の生成エラーを起こしている可能性がある。

【００２３】次に、２コヒーレント状態暗号について説明する。２コヒーレント状態暗号は２状態量子暗号の一例である。詳細は文献：[10] C.H.Benett,Phys.Rev.Lett.68,3121 (1992)、[11] B.Huttner,N.Imoto,N.Gisin,and T.Mro,Phys.Rev.A51,1863(1995) に述べられており、文献 [10] で提案された構成は図５に示すものであるが、説明のためにより簡略化した図４でまず説明する。

【００２４】図４において、送信者１は光パルス３を５０％のビームスプリッタ１０で光パルス１１と１２に分け、位相変調器１３を用いて光パルス１１の光位相を乱数表６に従ってビット値が“０”ならば０、ビット値が“１”ならば１８０度と変調し、光ファイバ１４と１５からなる量子チャンネル４に送る。以下すべての量子暗号において公開チャンネル５は共通であるので、以降本明細書では省略する。

【００２５】受信者２は、５０％のビームスプリッタ１６で光パルス１１および１２を干渉させる（実際は文献 [10] にも述べられているようにビームスプリッタ１０および１６の反射率は５０％である必要はない）。ビームスプリッタ１０からビームスプリッタ１６までは１つのマッハツェンダー干渉計を構成する。受信者２は光ファイバ１４と１５の間の位相差θを適当に調節し、ビームスプリッタ１６においてビット値“０”のパルスは受光器１７側がダークフリンジに、ビット値“１”のパルスは受光器１８側がダークフリンジになるようにする。

【００２６】２コヒーレント状態暗号では、光パルス３に含まれる平均光子数が１よりずっと小さい（例えば０．１の）コヒーレント状態の光を用いる。これは光パルス３に含まれる光子の数が２以上になる確率をできる限り０に近づけるためである。平均光子数が１よりずっと小さいので、パルス到着時に受光器１７と１８の何れにも光子がカウントされないケースがほとんどとなるので、ほとんどの場合受信者２にとってビット値判定不能となる。しかし、受光器１７でカウントされた場合はビット値は“１”、受光器１８でカウントされた場合は“０”であると確定的に結論することができる。以上のことから次のようなプロトコルで秘密鍵交換が可能であ

る。

【００２７】ステップ１：送信者１は乱数表６に従って光パルス１１の位相を位相変調器１３を用いて変調し、送る。

【００２８】ステップ２：受信者２は受光器１７と１８で光子のカウンティングを行う。カウントした場合、受光器１７と１８のどちらでカウントしたかは言わず、カウントした事実だけを公開チャンネルで送信者１に告げる。

【００２９】ステップ３：盗聴がないと仮定すれば、送信者は受信者が受光器１７と１８のどちらでカウントしたか知っているので、そのようなビット列から適当な割合で照合ビットを抽出し、それぞれの答合わせを（公開チャンネル５で）行う。十分な数の照合ビットが一致すれば、後で述べる理由により１に近い確率で盗聴されていないと結論づけられる。

【００３０】ステップ４：照合ビットを除いたビットは送信者１と受信者２しか知らない同一の値を有することが保証されているので、それを秘密鍵７と決定する。

【００３１】このスキームに対し盗聴者が何ができるかを考える。量子チャンネル４にアクセスして二手に分かれた光パルスの位相差を測定するためには、受信者と同様干渉させて光子カウンティングを行う必要がある。たまたまカウンティングに成功すれば、送信者と同じ装置を用いて送信者が送ったのと同じ並列２パルスを送ることができる。しかし、ほとんどのパルスで光子がカウントされないので、その場合は偽のパルスを何も送らないか、ランダムな位相差を持った偽のパルスを送るかしかない。前者の場合、伝送レートが本来値から下がり、後者の場合照合ビットの矛盾を引き起こし、いずれにせよ送信者と受信者から検知される。

【００３２】２コヒーレント状態量子暗号を実用化する際には、長い伝送路を含むマッハツェンダー干渉計において、伝送路の揺らぎによる位相差揺らぎをいかに安定化するかが重要となる。図４のように２本の光ファイバを用いたのでは５００ｍを越すあたりから干渉計の安定化は不可能となる［文献１２：井元信之「光子数の量子非破壊測定の研究」博士論文（東京大学）］。そこで光パルス１１と１２に時間差をつけて１本の光ファイバに通すことが考えられる［文献１０］。

【００３３】図５にその場合の構成を示す。図５において、送信者１は光パルス３を偏光ビームスプリッタ１９により直交する偏光関係にある等強度のパルス１１と１２に分ける。パルス１１を位相変調器１３で変調し、パルス１２はそのまま偏光ビームスプリッタ２０を介して偏光保存ファイバ４に入射する。このようにしてパルス１１と１２は遅延を持った二連パルスとして光ファイバ４の中を伝わり、受信者側では偏光ビームスプリッタ２１で二連パルスを分離し、逆遅延をかけた後、偏光ビームスプリッタ２２でパルス１１と１２を干渉させる。光パルス１１と１２は光ファイバ４の中を伝搬する間に同じ位相揺らぎを受けるので、干渉させるときには揺らぎが打ち消し合う。光ファイバの位相揺らぎの周波数特性は約１ＧＨｚまでと考えられるので、その揺らぎの影響を受けないためには、パルス１１と１２の間隔は１ｎｓ以下でなければならない。この場合の困難は、そのような極短二連パルスを可干渉性を失わないように発生することにある。

【００３４】次に、４コヒーレント状態暗号について説明する。４コヒーレント状態暗号は、上述した４偏光状態暗号と２コヒーレント状態暗号の特長を組合せ、いずれよりも大幅な性能改善を図ったものであり、詳細は文献１１に述べられている。構成的には図４の２コヒーレント状態暗号において位相変調を０度、９０度、１８０度、２７０度の４種類を用い、プロトコルとしては受信者が光子をカウントしたか否かの事実に加えて（０度、１８０度）のペアと（９０度、２７０度）のペアのいずれを選択したかを送信者と受信者が突き合わせるというプロトコルを付加した暗号である。詳しい動作および性能の比較は文献１１に詳しく解析されている。容易に推測されるように、この量子暗号法の欠点は上述した２コヒーレント状態暗号と同じ欠点を有している。

【００３５】次に、時間差干渉暗号について説明する。時間差干渉暗号は図４に示すようにマッハツェンダー干渉計を用いる点で図４の２コヒーレント状態暗号に類似しているが、他の量子暗号が非直交状態を用いるのに対し、直交する状態のみを用いる点が特徴的である。詳細は文献：［13］Goldenberg and Vaidmann:Phys.Rev.Lett.75,1239(1995) に述べられているが、以下簡単に説明する。図６に示すように、送信者１はビット“０”の場合はポートＡ側から、ビット“１”の場合はポートＢ側から光パルス３を入れ、乱数表６を送る。光パルス３は光子をただ１つ含むとする。光パルス３は５０％ビームスプリッタ１０で二手に分かれ、光パルス１１はそのまま光ファイバ１４に、光パルス１２は長い遅延２３を経て光ファイバ１５に入る。遅延を伝送距離より長くしておくことにより光パルス１１が受信者側に到着した後光パルス１２が伝送路部に入る。

【００３６】受信者側では光パルス１１に遅延２３と同じ長さの遅延２４を設ける。これにより５０％ビームスプリッタ１６において光パルス１１と１２は干渉し、ポートＡ側から入射した光パルス３はポートＡ’に、ポートＢ側から入射した光パルス３はポートＢ’に出射する。受信者２は単にポートＡ’かＢ’かを見ているだけで送信者１の乱数表６を再生できる。照合ビットの棄却や伝送損失による光子の欠落を除き、送信者と受信者は秘密鍵７を構築できる。盗聴者は伝送路部で光パルス１１と１２に同時にアクセスすることはできず、光パルス１１を測定・加工した後、光パルス１２を測定・加工することしかできない。文献１３に詳しく述べられている

通り、この制約の下ではビット“０”と“１”を破壊せずに読み取る手段がない。

【００３７】文献１３にも述べられている通り、この量子暗号は直交する状態のみを用いるという原理的興味で提案されたもので、実用性には乏しい。時間差を設けることが本質的であるので図５のような二連パルスを使うことができず、二本の伝送路を用いる以外にない。そのようなマッハツェンダー干渉計を安定化するためには伝送距離を数百m以下とせざるを得ない。

【００３８】次に、二光子干渉暗号について説明する。二光子干渉暗号はフランソン干渉計と呼ばれる二光子干渉計を利用する量子暗号で、文献：１４［A.E.Ekert et al.,Phys.Rev.Lett.69,1293（1992）］で提案された。図７はその動作を説明する図である。２４は光パラメトリック増幅器であり、角振動数ω_Pのポンプ光と呼ばれる光子２５を吸収し、角振動数ω_Aとω_Bの光子を１つずつ発生する。それぞれの光子パルスを２６および２７とする。光子パルス２６は光ファイバ２８に送られ、遅延２９を通過後受光器３０または３１でカウントされる。光子パルス２７は光ファイバ３２に送られ、遅延３３を通過後受光器３４または３５でカウントされる。遅延２９から先は送信者側、遅延３３から先は受信者側である。図のように送信者１と受信者２について対称な構成であるので、送信者あるいは受信者という名称は最良ではないが、他の量子暗号と用語を統一するためこれらの名称を用いる。位相差θ_Aは送信者側で調節し、位相差θ_Bは受信者側で調節する。光パラメトリック増幅器２４は送信者側と受信者側のいずれに回してもよいが、盗聴者はアクセスできないようにしておく。今、送信者と受信者が（$\theta_A+\theta_B=0$）となるように位相調整することを取り決めれば、フランソン干渉計の原理すなわち遠隔量子相関により、受光器３０と３５で光子が同時カウントされる確率や受光器３１と３４で同時カウントされる確率は０となる。従って受光器３０と３４で同時カウントがあるか、受光器３１と３５で同時カウントがあるか、あるいは同時カウントがないかのいずれかしか起きない。そこで、送信者と受信者が同時にカウントしたか否かのみを公開チャンネルで確認し合うだけで、送信者と受信者はそれぞれどの受光器でカウントしたかを互いに知る。このようにして共通の乱数表を構築できるので、ときどきビット照合して盗聴のないことを確認した残りのビットを秘密鍵として採用することができる。この方式では乱数表を用いて送信者が何らかの物理量を意図的に変調するプロセスはない。なぜならば、受光器３１と受光器３４で光子の同時カウントがあるか受光器３１と受光器３５で光子の同時カウントがあるかは、量子力学的確率過程として決まるからである。

【００３９】この量子暗号は実用的見地から優れた特徴をいくつか有している。まず、θ_Aとθ_Bが空間的にまったく独立であり、大きなマッハツェンダー干渉計の内部にあるわけではないので、伝送路の揺らぎと無関係に送信者と受信者が独立に調整できることである。また、偏光を使っていないので、任意偏光を保存する必要はなく、特定の偏光を保存する偏光保存ファイバを使うことができる。このためフランソン干渉計の安定化は極めて容易であり、しかも送信者と受信者が別個に安定化すればよい。

【００４０】この量子暗号の実用上の問題点は、遠く離れた送信者と受信者がカウントした光子が同時刻にカウントされたか遅延があったかを区別しなければならないことにある。遅延２８および３２はナノ秒のオーダーであるから（それ以上長くするとθ_Aやθ_Bの揺らぎを生ずる）、その程度の時間分解能で送信者と受信者のクロックを同期させる必要がある。これは一般に高価な設備を必要とする。

【００４１】

【発明が解決しようとする課題】上述したように、従来の量子暗号法のうち、４偏光状態暗号は、任意の偏光を保存するファイバを必要とするという問題がある。また、２コヒーレント状態暗号、４コヒーレント状態暗号、および時間差干渉暗号は、長距離マッハツェンダー干渉計の安定化を必要とし、更に二光子干渉暗号は、送信者と受信者間で高精度の同期クロックを必要とするという問題がある。

【００４２】本発明は、上記に鑑みてなされたもので、その目的とするところは、偏光を使用せず、遠隔量子相関を利用し、同時刻性測定を受信者側のみで行うことにより高精度同期クロックを必要としない量子暗号の構成方法を提供することにある。

【００４３】

【課題を解決するための手段】上記目的を達成するため、請求項１記載の本発明は、量子力学状態を変調した第１の信号を伝える量子チャンネルと、古典状態を変調した第２の信号を伝える古典チャンネルを用い、不確定性原理に基づいて盗聴行為によって前記第１の信号に発生する撹乱の有無を前記古典チャンネルで監視しながら、乱数表を送信側より受信側に伝送し、前記乱数表を秘密鍵とする量子暗号の構成方法において、送信側において、同一の時間幅を有し、前記時間幅より長いコヒーレント時間を有し、それぞれが１つの光子からなる第１および第２の光パルスを発生し、前記第１の光パルスを２つの光路に分岐し、分岐後の光パルスの一方に前記時間幅より長く前記コヒーレント時間より短い第１の時間遅延を施した後、分岐した他方の光パルスの光路に合流させ、合流した光路が取り得る２つの光路のうちの１つの光路を第１の量子チャンネルに光学的に接続し、前記第２の光パルスを第２の量子チャンネルに入力し、受信側においては、前記第１の量子チャンネルの出力を第１の光検出手段に入力し、前記第２の量子チャンネルの出力を２つの光路に分岐し、分岐後の光パルスの一方に、

前記第１の時間遅延との差が前記時間幅より小さい第２の時間遅延を施した後、分岐した他方の光パルスの光路に合流させ、合流した光路が取り得る２つの光路の一方を第２の光検出手段に入力し、他方の光路を第３の光検出手段に入力し、前記第１の光検出手段と第２または第３の光検出手段で信号が同時に検出され、しかも前記第１の時間遅延が与える位相差と第２の時間遅延が与える位相差が特定の組合せであったか否かを古典チャンネルにより確認し、特定の組合せであった場合のみ、１ビットの信号を登録することを要旨とする。

【００４４】請求項１記載の本発明にあっては、送信側において、第１および第２の光パルスを発生し、第１の光パルスを２つの光路に分岐し、分岐後の光パルスの一方に第１の時間遅延を施して、他方の光パルスの光路に合流させ、合流した光路が取り得る２つの光路のうちの１つの光路を第１の量子チャンネルに光学的に接続し、第２の光パルスを第２の量子チャンネルに入力し、受信側においては、第１の量子チャンネルの出力を第１の光検出手段に入力し、第２の量子チャンネルの出力を２つの光路に分岐し、分岐後の光パルスの一方に第２の時間遅延を施し、他方の光パルスの光路に合流させ、合流した光路が取り得る２つの光路の一方を第２の光検出手段に入力し、他方の光路を第３の光検出手段に入力し、第１の光検出手段と第２または第３の光検出手段で信号が同時に検出され、しかも第１の時間遅延が与える位相差と第２の時間遅延が与える位相差が特定の組合せであったか否かを古典チャンネルにより確認し、特定の組合せであった場合のみ、１ビットの信号を登録する。

【００４５】また、請求項２記載の本発明は、請求項１記載の発明において、前記第１および第２の光パルスを光パラメトリック増幅または原子のカスケード遷移によって発生することを要旨とする。

【００４６】更に、請求項３記載の本発明は、量子力学状態を変調した第１の信号を伝える量子チャンネルと、古典状態を変調した第２の信号を伝える古典チャンネルを用い、不確定性原理に基づいて盗聴行為によって前記第１の信号に発生する撹乱の有無を前記古典チャンネルで監視しながら、乱数表を送信側より受信側に伝送し、前記乱数表を秘密鍵とする量子暗号の構成方法において、送信側において、ポンプ光子を光パラメトリック増幅器に供給して、第１の光パルスおよび第２の光パルスを発生し、第１の光子パルスを２つの光路に分岐し、分岐された一方の光パルスに遅延手段で第１の時間遅延を施し、分岐した他方の光パルスの光路に合流させ、合流した光路が取り得る２つの光路のうちの１つの光路を光ファイバからなる第１の量子チャンネルに光学的に接続し、前記第２の光パルスを光ファイバからなる第２の量子チャンネルに入力し、受信側においては、前記第１の量子チャンネルの出力を第１の受光器に入力し、前記第２の量子チャンネルの出力を２つの光路に分岐し、分岐

された一方の光パルスに遅延手段により第２の時間遅延を施し、分岐した他方の光パルスの光路に合流させ、合流した光路が取り得る２つの光路の一方を第２の受光器に入力し、他方の光路を第３の受光器に入力し、前記第１の受光器と第２または第３の受光器で信号が同時に検出され、しかも前記第１の時間遅延が与える位相差と第２の時間遅延が与える位相差が特定の組合せであったか否かを古典チャンネルにより確認し、特定の組合せであった場合のみ、１ビットの信号を登録することを要旨とする。

【００４７】請求項３記載の本発明にあっては、送信側において、ポンプ光子を光パラメトリック増幅器に供給して第１の光パルスおよび第２の光パルスを発生し、第１の光子パルスを２つの光路に分岐し、一方の光パルスに第１の時間遅延を施し、他方の光パルスの光路に合流させ、合流した光路が取り得る２つの光路のうちの１つの光路を光ファイバからなる第１の量子チャンネルに光学的に接続し、第２の光パルスを光ファイバからなる第２の量子チャンネルに入力し、受信側においては、第１の量子チャンネルの出力を第１の受光器に入力し、第２の量子チャンネルの出力を２つの光路に分岐し、一方の光パルスに第２の時間遅延を施し、他方の光パルスの光路に合流させ、合流した光路が取り得る２つの光路の一方を第２の受光器に入力し、他方の光路を第３の受光器に入力し、第１の受光器と第２または第３の受光器で信号が同時に検出され、しかも第１の時間遅延が与える位相差と第２の時間遅延が与える位相差が特定の組合せであったか否かを古典チャンネルにより確認し、特定の組合せであった場合のみ、１ビットの信号を登録する。

【００４８】

【発明の実施の形態】以下、図面を用いて本発明の実施の形態について説明する。

【００４９】図１（ａ）は、本発明の一実施形態に係る量子暗号の構成方法を説明する図である。同図に示す本実施形態の量子暗号の構成方法は、フランソン干渉計の原理をベースに新しい量子暗号の構成およびプロトコルを考案したものであり、偏光を使用せず、遠隔量子相関を利用し、同時刻性測定を受信者側のみで行うことにより高精度同期クロックを不要にしたものであり、従来の二光子干渉量子暗号の優れた特徴をそのまま保有しているものである。

【００５０】図１（ａ）において、送信者１は光パラメトリック増幅器２４を用い、角振動数ω_Pのポンプ光子２５を角振動数ω_Aの光子２６と角振動数ω_Bの光子２７を発生する。光子２６は遅延２９を通過後光ファイバ２８に送り、光子２７はそのまま光ファイバ３２に送る。受信側では光子２６をそのまま受光器３１でカウントし、光子２７は遅延３３を通過後受光器３４または３５でカウントする。位相差θ_Aは送信者側で変調（固定調節でなくビット毎に）し、位相差θ_Bは受信者側で変

調する。その取り決めについては後述する。

【００５１】フランソン干渉計の原理、すなわち遠隔量子相関によれば、$\theta_A+\theta_B$が０または１８０度の場合は、同時カウントがあるとすれば受光器３１と３４に限られ、$\theta_A+\theta_B$が９０度または２７０度の場合は、同時カウントがあるとすれば受光器３１と３５に限られる。この事実を用いることにより、４偏光状態暗号プロトコルと類似のプロトコルを用いて量子暗号を実現することができる。

【００５２】まず、送信者１は二種類の変調法から１つを選択する。変調法１ではビット“０”のときθ_A＝０、“１”のときθ_A＝１８０度とし、変調法２ではビット“０”のときθ_A＝９０度、“１”のときθ_A＝２７０度とする。変調法１と２に対応し、受信者側では復調法１としてθ_B＝０、復調法２としてθ_B＝９０度のうちから選択する。送信者と受信者の選択の可能な組合せに対し同時カウントが起こり得る受光器のペアを図１（ａ）に示した。この図から、送信者の変調法と受信者の復調法が一致した場合にのみ、同時カウントのある受光器ペアが一意に定まることが分かる。変調法と復調法が一致しない場合は情報の伝達が行われない。具体的プロトコルは次の通りである。

【００５３】ステップ１：送信者１はランダムに変調法を選択し、乱数表６に従ってθ_Aを変調する。

【００５４】ステップ２：受信者２は送信者１と独立にランダムに復調法を選択し、θ_Bを設定する。受光器３１と３４または３１と３５のいずれかのペアで光子の同時カウントが起こり得る。

【００５５】ステップ３：同時カウントを観測する毎に（あるいは後でまとめて交信してもよいが）受信者２はどちらの復調法を選択したか、公開チャンネルで明らかにする。送信者１はそれを聞き、受信者２の復調法選択が正しかったか否かを受信者２に明らかにする。

【００５６】ステップ４：送信者１と受信者２は双方が対応する変復調法を選択した約半分のビットだけを採用し、後の半分は捨てる。盗聴がなければ双方に同じ乱数表が形成されているはずである。

【００５７】ステップ５：送信者１と受信者２は残ったビットのうち適当な割合で照合ビットを抽出し、それぞれの答合わせを行う。十分な数の照合ビットが一致すれば１に近い確率で盗聴されていないと結論づけられる。

【００５８】ステップ６：照合ビットも除いたビットは送信者１と受信者２しか知らない同一の値を有することが保証されているので、それを秘密鍵７と決定する。

【００５９】

【発明の効果】以上説明したように、本発明によれば、位相差θ_Aとθ_Bが空間的にまったく独立で伝送路の揺らぎと無関係に送信者と受信者が独立に調整できるので、長距離マッハツェンダー干渉計の安定化のような送信者と受信者を包括して調整を行う必要がない。また、偏光を使っていないので、任意の偏光を保存する光ファイバを要求しない。更に、本発明では光子の同時カウントを受信者側のみで行うため、受信者がローカルなクロックを持っていればよい。これは送信者と受信者の間で高精度の同期クロックが必要であった従来の二光子干渉量子暗号と大きく異なる点である。このように、本発明は上述した従来の量子暗号の欠点をすべてクリアする新しい量子暗号の構成方法を実現することができる。

【図面の簡単な説明】

【図１】本発明の一実施形態に係る量子暗号の構成方法を説明するための図および本実施形態における光子の同時カウンティングがあり得る受光器対を示す図である。

【図２】従来の量子暗号である４偏光状態暗号を説明するための図である。

【図３】図２に示す４偏光状態暗号におけるコーディング法およびビット値との対応する偏光状態を示す図である。

【図４】従来の量子暗号である２コヒーレント状態暗号を説明するための図である。

【図５】従来の量子暗号である２コヒーレント状態暗号を説明するための図である。

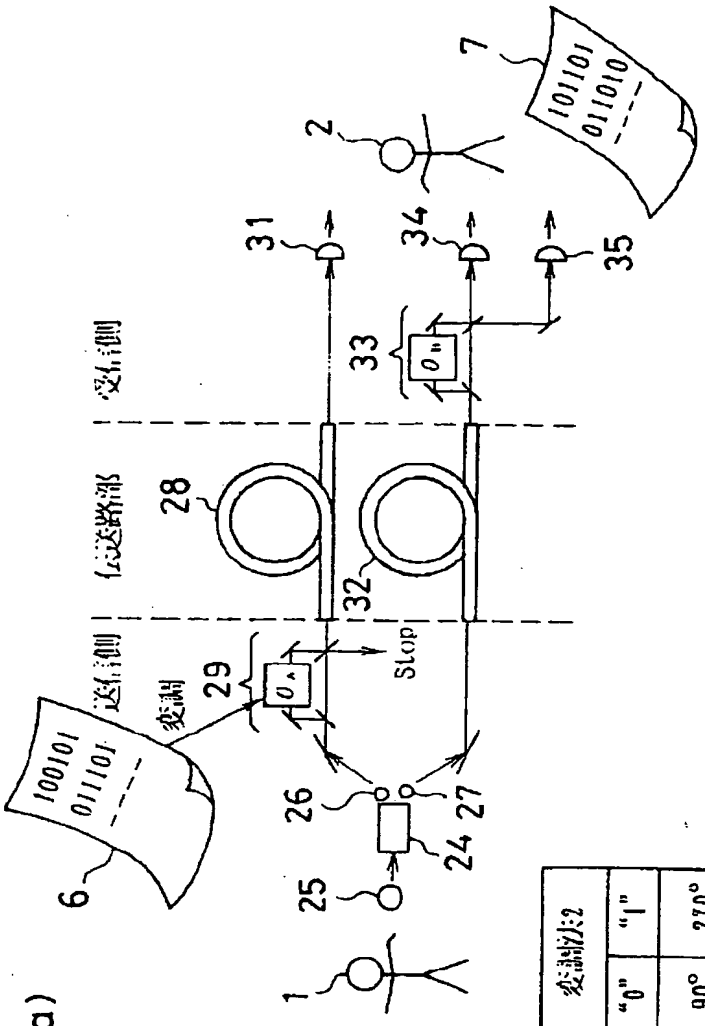
【図６】従来の量子暗号である時間差干渉暗号を説明するための図である。

【図７】従来の量子暗号である二光子干渉暗号を説明するための図である。

【符号の説明】

１　送信者
２　受信者
２５　ポンプ光子
２８，３２　光ファイバ
２９，３３　マッハツェンダー型遅延
３１，３４，３５　受光器

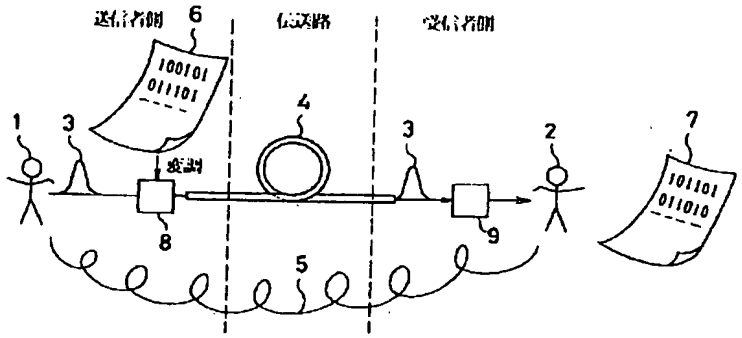
【図1】



(b)

送信者の変調法 / 受信者の復調法		変調法1		変調法2	
		"0"	"1"	"0"	"1"
	O_A / O_B	0°	180°	90°	270°
復調法1	0°	31と34 0Hz	31と35 0Hz	31と34 31と35	31と34 31と35
復調法2	90°	31と34 31と35	31と34 31と35	31と35 0Hz	31と34 0Hz

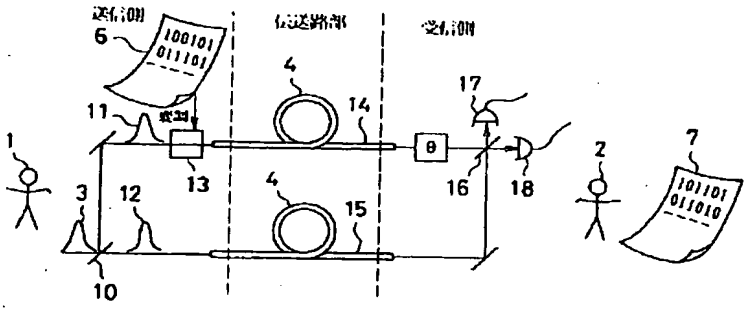
【図２】



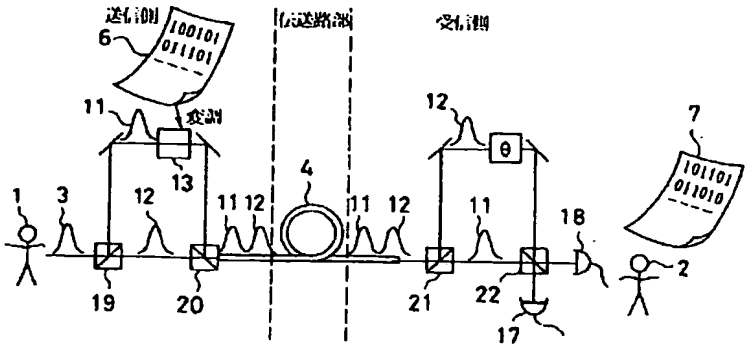
【図３】

	ビット "0"	ビット "1"
直線偏光コーディング	↔	↕
円偏光コーディング	○	○

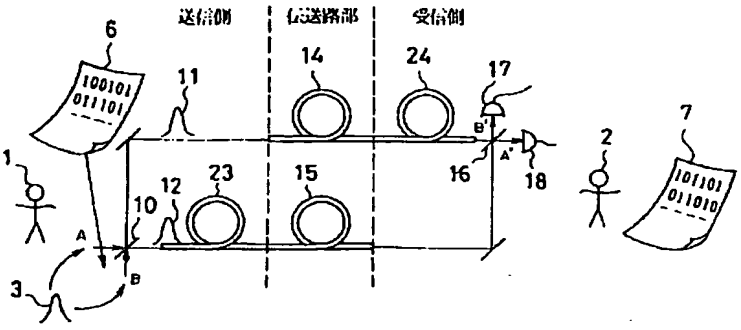
【図４】



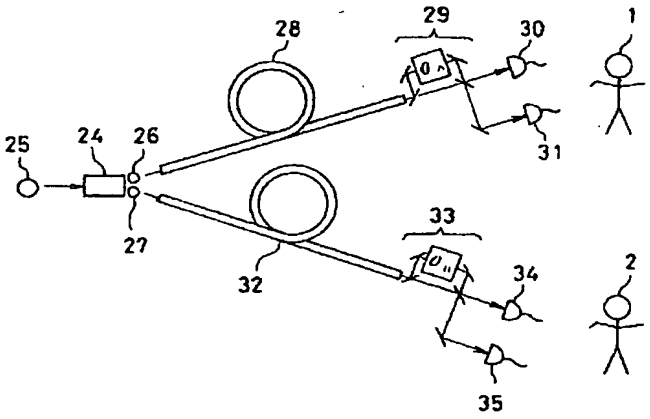
【図５】



【図６】



【図７】



フロントページの続き

(51)Int.Cl.⁶		識別記号	庁内整理番号	F I		技術表示箇所
H04L	9/08			H04L	9/00	601C
	9/38					691